Claim 11

A user authentication system comprising:

the user authentication apparatus for said prover computer according to claim 9; and

a plurality of user authentication apparatuses for said verifier computers according to claim 10.

Claim 12

A user authentication system, wherein a one-way function F, which should satisfy $v = F(g, -s)$, is determined by employing an integer g, which is defined in advance, for the relation between a public key v and a secret key s of a prover computer, and wherein a relation is verified between said prover computer and each of multiple verifier computers, comprising:

transmission means, for said prover computer, for generating a random number a and obtaining a cryptogram $A =$ the function $F(g, a)$, and for transmitting said obtained cryptogram A to said verifier computers;

reception means for said verifier computers, for receiving said cryptogram A from said prover computer;

transmission means for said verifier computers, for generating a random number b with which said cryptogram A is employed to obtain a cryptogram $B =$ the function $F(g, b)$ and a cryptogram $X =$ the function $F(A, b)$, and for transmitting said cryptograms B and X to said prover computer;

reception means for said prover computer, for receiving said cryptograms B and X from said verifier computers;

verification means for said prover computer, for employing said cryptograms B and X to determine whether a relation of said cryptogram X = the function F(B, a) has been established;

cryptogram computation means for said prover computer, for generating a random number c when it is ascertained that said relation has been established, and for obtaining said cryptogram C = the function F(g, c) and said cryptogram Y = the function F(B, c), or said cryptogram C = the function F(A, c) and said cryptogram Y = the function F(X, c), and a cryptogram Z = the function H(a, Y, s); and

cryptogram transmission means for said prover computer, for transmitting said cryptograms C, Y and Z to said verifier computers;

cryptogram reception means, for said verifier computers, for receiving said cryptograms C, Y and Z from said prover computer; and

verification means for said verifier computers, for employing said cryptograms C, Y and Z that are received to verify a relation between said verifier computers and said prover computer when two relations of said cryptogram Y = the function F(C, b) and said cryptogram A = the function J(v, Y, g, Z) are established at the same time.

13. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing user authentication, the

computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the apparatus of claim 9.

14. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing user authentication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the apparatus of claim 10.

15. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing user authentication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the system of claim 11.

16. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing user authentication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the system of claim 12.

17. An article of manufacture comprising a computer

usable medium having computer readable program code means embodied therein for implementing a user authentication method, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.